(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 September 2003 (04.09.2003)

PCT

(10) International Publication Number
WO 03/073353 A2

(51) International Patent Classification[7]: G06F 19/00, 19/00

(21) International Application Number: PCT/SG03/00026

(22) International Filing Date: 4 February 2003 (04.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10/067,493	4 February 2002 (04.02.2002)	US
PCT/GB02/01750	15 April 2002 (15.04.2002)	GB
200205416-1	6 September 2002 (06.09.2002)	SG

(71) Applicant *(for all designated States except US)*: **MSC HEALTHCARE PTE. LTD.** [SG/SG]; 29/31 Gul Avenue, Singapore 62966 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SIONG CHEAK, Steven,, Mok** [SG/SG]; Blk 682C Jurong West Central 11, #09-130, Singapore 64368 (SG). **TECK KEONG, Bong** [SG/SG]; Blk 204, Jurong East Street 21, #04-255, Singapore 60020 (SG).

(74) Agent: CHONG, Y., F.; W.P.AI & Company, PSA BLDG, P.O. Box 0399, Singapore 911144 (SG).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/073353 A2

(54) Title: SMART CARD FOR USE WITH HEALTH CARE INSTITUTIONS AND FINANCIAL INSTITUTIONS

(57) Abstract: A smart card (10) for use with members of a Healthcare Exchange (20), the smart card having a first identifier (11) containing encrypted data; a second identifier (12) with credit card data of a smart card holder; and a memory for storage, in encrypted code, of an electronic medical record ("EMR") of the smart card holder. The smart card also has an emergency number (13) for access to a website containing a summary page of predefined information of the smart card holder and an 1800-xxx or 1900-xxx phone number (14) on the card for calling a 24x7 call center, to obtain a full health or medical history on the smart card holder. A system which enables the Healthcare Exchange (20) to capture financial information arising from transactions using the smart card is also disclosed. The financial information is sent to the Credit Card Company which issued the second identifier (12) for consolidation with other financial information on transactions made by the smart card holder using another credit card or a debit card issued by the same Credit Card Company.

TITLE OF THE INVENTION

SMART CARD FOR USE WITH HEALTH CARE INSTITUTIONS AND FINANCIAL INSTITUTIONS

FIELD OF THE INVENTION

The present invention discloses a method and apparatus for a smart card which can be used on card readers of health care providers belonging to a healthcare exchange (disclosed in US Application No. 10/067,493 and PCT/GB02/01750 filed by the present applicant) and card readers operated by financial institutions such as credit card companies. The smart card having two identifiers, each identifier operable with different types of identifier readers during a transaction with a healthcare provider, generating two sets of financial and other data, said financial data relating to each transaction generated from different identifiers being consolidated in a single billing statement issued by the financial institution to the smart card holder.

DESCRIPTION OF THE RELATED ART

An identifier embedded in a card such as a Credit Card are commonly found. An identifier refers to a magnetic strip attached to a credit card or an smart chip embedded in the credit card. Such identifier facilitates authentication on an identity against a payment network's database thereafter enables a credit service. These payment networks include financial institutions such as Visa ®International, MasterCard®, American Express®, etc.

Other common forms of implementing some form of an identifier on a card includes: ATM card, Debit card, CashCard, Loyalty card, etc. In most of these cards, such identifier served as an authentication mean and/or further store some simple strings of data representing a cash value or an accumulated loyalty value.

However, each of these identifiers are implemented by the issuer of the proprietary card, using its own proprietary system and payment network. The system of each card issuer is therefore incompatible with one another. As a result, lots of general billing notices or billing statements from each system need to be generated and physically mailed to a particular user if he or she signs up with the issuers of a few cards. It is therefore common for a consumer to hold several types of cards and to receive one statement from each one of service providers or card companies.

Lately, there has been efforts to integrate two identifier on a card (i.e. CreditCard smart chip and CashCard smart chip), in which only one of the identifiers has a payment network, connecting with merchants, banks and settlement bank), while the other identifier merely serves as storage of a simple cash value.

In attempt to solve the problem of many statements from various card companies, efforts have also been directed at merging two payment network structures. However, this has proved almost impossible due to the fact that each of the payment network has its own unique process flow operable in accordance to the nature of its business model and industry.

Another effort in merging billing records has been described in US5684965 and US5483445, which disclosed an automatic billing system by a payment network to consolidate many utility bills under its billing statement.

Use of smart cards in healthcare systems are also known. PCT/US00/19706 describes a patient healthcare record system for storing, managing and retrieving healthcare information via a smart card such smart card having a processor or chip and at least one file.

PCT/US01/08291 describes use of tokens including a smart card to store patient biographical information and emergency medical information. The token or smart card is used to authorize access to a remote database of patient medical information by base units operated by various types of healthcare professionals.

Efforts to improve data capture in the provision of healthcare services for processing healthcare claims have also been made. An example is US Application No. 10/011,96. However, the data capture is by means of hand held computers.

PROBLEM TO BE SOLVED BY THE INVENTION

In the provision of healthcare services, there are many parties involved such as health care providers, pharmacies, medical practitioners and specialists, healthcare equipment suppliers, nutritional food specialists, nursing care centers, medical research laboratories, medical distribution and delivery services, emergency services providers, health care libraries, hospitals, insurers and credit/debit card issuer, all of which belongs to a healthcare exchange, and all of whom serve the health care receipient. Such a Healthcare system has been disclosed in US Application No. 10/067,493 and PCT/GB02/01750 filed by the present applicant.

The health care receipient would usually be a member of or subscriber to a healthcare or health insurance programme managed by a Managed Care Organization. Provision of healthcare services would be through identification of the healthcare receipient by authentication of a smart card. It can be seen that the statements generated by each of the healthcare providers to the smart card holder are numerous.

It is therefore desirable for the smart card holder to receive a consolidated statement for all the services provided. It is even more desirable if the smart card holder receive from the credit card company a consolidated statement listing all transactions for purchase of services and goods including transactions relating to healthcare services provided through the Healthcare Exchange, and such statements also containing other information on the status of the smart card holder's healthcare policies .

MEANS TO SOLVE THE PROBLEM

The present invention discloses a method and apparatus for a Healthcare Exchange to implement a smart card System, in which the smart card

comprises an authentication mean to authenticate an identity against a credit payment network over a secured network (Internet), another authentication mean to authenticate an identity against a healthcare exchange over a secured network (Internet); and a memory to store electronic medical record. The identifiers on the smart card, are operable with different types of identifier readers during a transaction with a healthcare provider. Thereafter the financial data relating to the transactions with all care providers are consolidated for billing purposes, by a financial institution such as credit card company in a single billing statement which is then issued to the smart card holder.

Further, the present invention discloses a method and apparatus for a Healthcare Exchange to implement a Card System, in which at least an emergency number (access code or the card number) is printed on the card. During an emergency situation, this number can be used as the login number to access a summary page of predefined information relating to the cardholder, such as critical health data, allergy, next-of-kin's particulars, etc through a web browser. In the present context, the summary page is named as " emergency page " or "e-page".

Next, the present invention discloses a method and apparatus for a Healthcare Exchange to implement a Card System, in which at least an 1800-xxx or 1900-xxx phone number is printed on the card. This number is connected directly to a 24x7 call center, wherein during an emergency, the helpdesk will be able to provide a full health or medical history relating to the cardholder through a web browser or fax machine after a secured authentication process.

SUMMARY OF THE INVENTION

A first object of the invention is a smart card operable with a card reader for use in a healthcare provider registered with a Healthcare Exchange, the smart card having:-

a first identifier containing encrypted data ;

a second identifier with credit card data of a smart card holder; and

a memory for storage, in encrypted code, an electronic medical record ("EMR") of the smart card holder

and in which the first identifier is capable of authenticating the identity of the smart card holder against the Healthcare Exchange over a modem dial-up or dedicated network (Internet) access and the second identifier is capable of authenticating the identity of the smart card holder against a credit payment network over a modem dial-up or dedicated network (Internet) access during a transaction with the healthcare provider.

A second object of the invention is smart card having these additional features:-

an emergency number which is either the access code or the card number which during an emergency situation, this number can be used as the login number to access a summary page of predefined information relating to the smart card holder, such as critical health data, allergy, next-of-kin's particulars, etc through a web browser; and

an 1800-xxx or 1900-xxx phone number printed on the card for calling to a 24x7 call center, wherein during an emergency, the helpdesk will be able to provide a full health or medical history relating to the smart card holder through a web browser or fax machine after a secured authentication process over the telephone.

for use in an emergency encountered by the smart card holder either to obtain assistance from a healthcare provider registered with the Healthcare Exchange or from any medical institution.

Preferably, the first identifier in the smart card is a smart chip or a JAVA smart chip.

Preferably, the second identifier containing credit card data of the smart card holder is a bar code, magnetic strip, smart chip or a JAVA smart chip issued by a Credit Card Company and the said Credit Card Company has also issued a credit card or debit card to the same smart

card holder.

Preferably, the second identifier containing credit card data of the smart card holder can be a bar code, magnetic strip, smart chip or a JAVA smart chip issued by a financial institution such as a Credit Card Company and of which the smart card holder is registered with.

Preferably, the first identifier stores the following data:-

General healthcare data including drug allergies and healthcare user's particulars including emergency contact number, body mass, height, blood group etc;

Physician's advice and medical treatment of the last 5 to 30 clinical Visits or more;

Real time data gathered from the sensing modules of remote monitoring device (includes blood pressure, SPO2, blood glucose, pulse rate, body temperature and ECG); and

Encrypted password for identity authentication.

which upon successful authentication of the first identifier, the data stored in the first identifier would be checked with a database of the Healthcare Exchange for the latest update or vice versa; and the latest record will always replace only the oldest record in the first Identifier of the smart card while the latest record will be uploaded and archived in the database of the Healthcare Exchange.

Preferably, on successful authentication of the first identifier with the Healthcare Exchange and upon the EMR stored in the Healthcare Exchange being compared with the EMR stored in the Healthcare Exchange, the updating of the EMR would include the financial information on transactions arising from use of the smart card including installments under managed care plans, purchases of supplies and services from service provider members of the Healthcare Exchange, purchases of

medical services not covered by the managed care plans of the smart card holder and including any credits due to the smart card holder.

Preferably, the financial information on the transactions of the smart card with the Healthcare providers of the Healthcare Exchange are transmitted over a modem dial-up or dedicated network (Internet) access to the database of the Healthcare Exchange and stored by the Healthcare Exchange and at the end of a billing cycle, the financial information on the transactions of the smart card being sent to the Credit Card Company and the said financial information is consolidated with other financial information on transactions made by the smart card holder using the second identifier of the smart card and a credit card or a debit card issued by the same financial institution that issued the second identifier.

Preferably, the financial information on the transactions with healthcare providers of the Healthcare Exchange using the first identifier of the smart card and financial information on transactions of the second identifier of the smart card and the credit card or debit card of the smart card holder are consolidated by the same Credit Card Company which issued the second identifier, the financial information being presented to the smart card holder in one consolidated billing statement issued by the Credit Card Company for settlement by the smart card holder.

Preferably, the smart card is operable with a card reader installed in a Public Kiosk offering remote health monitoring services or a card reader installed in a personal computer or in a note book or a PDA or e-tablet or mobile phone and which is connected by a modem dial-up or dedicated network (Internet) access wherein upon successful authentication of the first identifier, the smart card holder would be able to access the website of the Healthcare Exchange for information on EMR of the smart card holder, for access to Telemedicine services, for access to On-line Disease management, access other Healthcare applications such as billing status, making of appointments with healthcare providers and general enquiries and Healthcare user education and programmes for health maintenance .

Preferably, the smart card is operable with a card reader installed in a device operated by a healthcare provider registered with the Healthcare Exchange or in a device installed in a public kiosk wherein the device could be a remote monitoring device, a massage chair or a treadmill and the smart card holder would receive healthcare service such as monitoring of blood pressure, SPO2, body temperature, pulse rate, blood glucose and ECG, or massage or a heart check.

Preferably, the smart card is operable with a card reader installed in a Public Kiosk offering Internet services or a card reader installed on a personal computer or a note book or e-tablet or a PDA or mobile phone and which is connected to a modem dial-up or dedicated network (Internet) access wherein upon successful authentication of the first identifier, the smart card holder can view the latest data available on the smart card holder's managed care plans or health insurance plans over the Internet.

Preferably, the smart card is operable with a card reader installed in a device operated by a healthcare provider registered with the Healthcare Exchange wherein the smart card could be used to receive medical care services such as hospital stay and treatment, nursing care, pharmaceutical supplies, medical treatment and consultation by medical specialists and general practitioners, nutritional food and healthcare products, supplies from healthcare library, suppliers of medical devices and equipment, laboratory tests reports and other services undertaken by Healthcare Exchanges.

Preferably, the smart card can also be used for transactions with a healthcare provider without a card reader installed by a payment network whereby the first identifier in the smart card is used on the card reader and upon authentication, the financial information arising from the transaction with the healthcare provider is transmitted over a modem dial-up or dedicated network (Internet) access to the database (21) in the Healthcare Exchange and stored in the said database and at the end of a billing cycle, the said financial information is sent to the Credit Card Company and consolidated with other financial information on

transactions made by the smart card holder using the second identifier of the smart card or another credit card or a debit card issued by the same Credit Card Company.

A third object of the invention is a system for capturing financial information arising from transactions using a smart card of this invention wherein the financial information is transmitted by a modem dial-up or dedicated network (Internet) access from the card reader installed in the healthcare provider to the database of the Healthcare Exchange and at the end of a billing cycle, the financial information are sent by the Healthcare Exchange to the Credit Card Company which issued the second identifier and thereafter, the said financial information is consolidated by the same Credit Card Company with other financial information received by the same Credit Card Company on transactions made by the smart card holder using the second identifier of the smart card or another credit card or a debit card issued by the same Credit Card Company to the same card holder.

A fourth object of the invention is a system for capturing information for EMR of a smart card holder for use in a Healthcare Exchange from card readers installed in devices such as Personal Computer, Public Kiosk, a remote Health monitor, a massage chair or a treadmill whereby a smart card holder would receive healthcare services and information stored in the first identifier would be checked with a database of the Healthcare Exchange for the latest update or vice versa; and the latest record will always replace only the oldest record in the first Identifier of the smart card while the latest record will be uploaded and archived in the database of the Healthcare Exchange.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the invention, its advantages, and the objects attained by its use, reference should now be made to the accompanying drawings. The accompanying drawings illustrate one or more embodiments of the invention and together with the description herein, serve to explain the workings and principles of the invention.

Figure 1 shows use of the smart card of the present invention in the healthcare network of service providers and a Health Care Portal which is collectively referred to as the Healthcare Exchange. The Healthcare Exchange is managed by the MCO. The workings of such a Healthcare system has been disclosed in US Application No. 10/067,493 filed on 04.02.2002 and PCT/GB02/01750 filed on 15.04.2002 in the name of the present applicant.

Figure 2 depicts the features of the smart card of the present invention.

Figure 3 shows a process flow relating to a billing process due to a transaction.

Figure 4 illustrates a schematic diagram of communication flow between a card and a network/ or exchange.

Figure 5 presents another embodiment of the smart card depicted in Figure 4.

Figure 6 depicts a billing process flow of the card system for the present invention.

Figure 7 shows that the smart card of the present invention can be used in any card reader installed in a plurality of devices or equipment and which is integrated with a healthcare identifier reader, and connected with a healthcare exchange. These devices could be a simple card reader module to be used in a retail shop; Public kiosk; Device in public transportation; A computer module; Daily appliances (including sofa chair); Portable monitoring device; and . Electronic communication devices.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 shows how the smart card of the present invention is used in relation to the healthcare network of service providers and a Health Care

Portal (30) which is collectively referred to as the Healthcare Exchange (20). Part of the Healthcare Exchange would also include the credit card issuer or financial institution and Health and Medical Insurance companies. The entire Healthcare Exchange (20) is managed by a Managed-Care Organisation (referred to as " MCO ") which is supported by a management team, backed by accounting and audit services. The MCO would be the organization responsible for management, control and maintenance of a electronic medical and Health care record database referred to in this invention.

The Health Care Portal (30) provides on-line services such as Electronic Health Care & Medical Record Management (referred herein as " EMR Management "), Real-time Health Care consultation (also known as " Telemedicine "), Real-Time Health Care Monitoring, Feedback & Activation (also known as " On-line Disease Management "), Health Care application (such as Billing, appointments, status enquiry) and Health Care Education (offering on-line health education programmes).

The services taken up by a smart card holder may include visits and consultations to any of the health care providers, purchases of services and goods from the health care providers, including outpatient and in-patient services and intensive care services.

The healthcare service providers would include hospitals, nursing care centers, medical device/medical equipment suppliers, clinical management systems, drug and pharmacy suppliers, emergency services, healthcare device/healthcare equipment suppliers, nutritional food suppliers, Healthcare libraries, Medical Research Laboratories and Specialists, Government departments in charge of healthcare, medical insurance schemes, Medication distribution and Delivery services.

Typically of the modern day healthcare exchange, the healthcare user is usually covered by some form of medical insurance scheme either on a voluntary basis or under the auspices of a Government or Statutory Authority. Settlement of the charges for the healthcare services are likewise made in a number of ways, including by charges to credit

cards. It can be seen that healthcare transactions initiated by the smart card holder with the providers of the healthcare services would finally be settled by credit card companies and insurance companies in one form or other.

For such a network, use of the smart card of the present invention would allow authentication of an identity to:

- Access into electronic medical record (EMR);
- Acquire on-line healthcare consultation or diagnostics with a healthcare call center;
- Acquire on-line disease management and monitoring through a portable monitor, massaging chair or public kiosk, in which all of these means are integrated with healthcare sensors;
- Make a payment, make an appointment with a healthcare provider, request for information, monitor a status of a healthcare application;
- Interact or participate in a personalized healthcare educational programme (known as Take Charge Programme or other educational programmes);
- Interact with any of the healthcare providers in the exchange;
- Retrieve e-page with the emergency number through the web browser; and
- Request for detail medical/ health history of the cardholder with 1800-xxxxxxx or 1900-xxxxxxx from a call center.

Fig. 2 depicts the features of the smart card (10) of the present invention. The features of the card includes:-

A first identifier (smart chip) (11) which serves as an authentication means for connection to a Healthcare Exchange (20) and a memory to store EMR;

A second identifier (magnetic strip) (12) which serves as an authentication means for connection to a payment network;

An emergency number (13) to retrieve an "e-page" from a healthcare

exchange through the web browser (Strictly for emergency situation); and

An 1800-xxxxxxx or 1900-xxxxxxx phone number (14) connecting to a 24x7 call center to request for full details of health/ medical record of the particular cardholder (which is strictly for emergency situations).

The storage of the first identifier is partitioned into 4 sectors, which respectively store:

(a) General healthcare data (drug allergy) and healthcare user's particulars including emergency contact number, body mass, height, blood group etc;

(b) Physician's advice and medical treatment of the last 5 to 30 clinical visits or more (latest record will replace the oldest one/and will check with MCO database for the latest update or vice versa);

(c) Real time data gathered from the sensing modules of remote monitoring device (includes blood pressure, SPO2, blood glucose, pulse rate, body temperature and ECG); and

(d) Encrypted password for identity authentication.

It is customary to refer to (a)-(c) as "EMR" and this is the definition given herein whenever reference is made to " EMR".

Fig. 3 illustrates a schematic diagram of communication flow between a card and a network/ or exchange.

The first identifier comprises of a READ and WRITE memory and/ or microprocessor. The first identifier can also be a Java chip. The first Identifier has its minimal function of identity authentication. The first identifier also has a memory for the further function of recording a transaction in accordance to date, time and the assigned code number of the reader. The first identifier has further memory functions of storing data, wherein the data is not limited to user's particulars, critical medical data, electronic medical record

(EMR), Insurance record, real-time healthcare data measured by a healthcare monitoring device, loyalty point/ value, etc. The data in the entire memory of the first identifier is referred to as " encrypted code A ".

The second Identifier can be a barcode, magnetic strip, smart chip or a JAVA smart chip. The identifier has a memory for data relating to the credit card information of the smart card holder and is referred to as " encrypted code B ".

The smart card has an emergency number (code/It can be the card number) printed on the card. During an emergency situation, this number can be used as the login number to access a summary page of predefined information relating to the cardholder, such as critical health data, allergy, next-of-kin's particulars, etc through a web browser. In the present context, the summary page is named as " emergency page " or "e-page".

The smart card has an 1800-xxx or 1900-xxx phone number printed on the card. This number is connected directly to a 24x7 call center, wherein during an emergency, the helpdesk will be able to provide a full health or medical history relating to the cardholder through a web browser or fax machine after a secured authentication process over the telephone.

Figure 4 shows a process flow relating to the billing process arising from a typical transaction with the Healthcare Exchange. Fig. 4 shows the communication flow between a smart card and the network of healthcare providers and the Healthcare exchange and the payment network. In this example, the smart card (10) has a chip for the first identifier (11) and a magnetic strip for the second identifier (12).

Figure 5 shows a process flow relating to the billing process arising from a typical transaction with the Healthcare Exchange wherein the smart card (10) has a chip for the first identifier (11) and a second chip (15) instead of a magnetic strip for the second identifier. Again, Fig. 5 is similar to Fig. 4 and shows the communication flow between a smart card and the network of healthcare providers and the Healthcare exchange and the payment network.

Referring to both Fig. 4 or 5, whatever form of smart card is used, a typical transaction from an identifier for a healthcare exchange, in a sequential manner would be described.

A typical transaction comprises the smart card holder's acquisition of healthcare services and/or goods from a health care provider. The smart card could be used for purchase of goods such as medicines from a pharmacy or leasing from a portable monitoring devices or purchase of specialist medical services or even for admission to a hospital for in-patient services or intensive care.

Referring to Fig. 4, at the point of initiation, the smart card holder would submit his smart card (10) to the service provider or retailer of medical goods or services, who would be part of the Healthcare exchange (20) for authentication and update of data. For illustration purpose, assume the service to be purchased by the smart card holder is a medical consultation. A contact or contactless communication is then initiated between the identifier and its dedicated reader, followed by providing a password on a keypad or fingerprint on a bio-metric reader. Encrypted code B is stored in the memory of second identifier while encrypted code A and EMR are stored in the memory of first identifier.

When a healthcare identifier is inserted/or swapped on its reader, encrypted code A will be sent from the memory to the database of MCO (21) for an authentication process. Thereafter, if the authentication is successful, both EMRs stored in the card and in the database of MCO will be compared with respect to their dates of modification. Only the oldest in the first Identifier of the smart card would be updated while the latest record will be uploaded and archived in the database of the Healthcare Exchange. This is to keep all histories relating to a patient (the smart card holder) as an audit trail in the database of the MCO. It must be pointed out that no one is authorised to delete or overwrite any record in the database of the MCO.

The updates upon successful authentication would include the credits if any, due to the smart card holder. If there is no available

credits, the smart card holder would be informed by the service provider (through the MCO) that the service to be provided has to be settled by the smart card holder on his own account. If the service to be purchased is a consultation with a medical specialist, the use of the smart card would enable the medical specialist to obtain the latest medical data on the smart card holder. After consultation, the latest EMR would be uploaded to the database of the MCO (21) via the internet through the system of the service provider. A newer copy of the EMR would also be updated into the smart card simultaneously after the consultation.

Now, after the consultation, the smart card holder have to pay for the services. If the smart card holder may have sufficient credits in his account (arising from his insurance policies), he may not have to make any payment. Although no payment is made by the smart card holder, the services of the healthcare provider is now to be settled by the MCO. In this case, the healthcare provider's claim is submitted to MCO. Verification of claim would be made at least against the transaction captured in the exchange. An approval or rejection of the service by MCO on the claim would be made. In turn, the MCO would submit the payment to the Insurer (only for those transactions insured under the reinsurance policy between MCO and Insurer). Approval or rejection of this claim by Insurer would now be made.

If the smart card holder has utilized his credit under his medical or health insurance scheme, he would be informed by the MCO to settle the charges on his own account.

If the card holder has no credits under his managed care plan, he can still use first identifier to record his acquisition of service. There are also occasions when the smart card holder receives some service not covered under his managed care plan from some clinics or healthcare providers without any credit card reading facility. In this case, the smart card holder could use the smart card to record his acquisition of service. For such cases, after the provision of service, another contact or contactless communication would then be initiated, this time between the first identifier and its dedicated reader, followed by providing a password on a keypad or

fingerprint on a bio-metric reader; Encrypted code A is stored in the memory of first identifier would be verified. The financial data from the transaction will be generated and stored by database of the MCO. Subsequently the same financial data would be transmitted by the MCO to the credit card center for billing consolidation. In this way, the sum charged for the service would be settled by the smart card holder in the usual procedure when the smart card holder receives his statement from his credit card company at the end of the billing cycle.

The present invention therefore offers the flexibility of using the smart card to acquire services from the healthcare provider when either the healthcare providers do not have any credit card reading facility or when the smart card holder receives services not covered by his managed care scheme.

If the smart card holder has to pay for the services, the smart card is again used. When the second identifier (12), being a CreditCard identifier, is inserted/or swapped on its reader, encrypted code B will be sent from the memory to Credit Payment Network for an authentication process. Thereafter, if the authentication is successful, the smart card holder would settle the charges for the services rendered by charging the costs of the service to his credit card account. The authentication process by the credit card company being a well established procedure would not be described herein. Similarly, the processing of the credit card charge and related approval process being a well established procedure would not be described herein. The record of the transaction would then be captured by the credit card company. At the end of each billing cycle, the credit card company would consolidate the credit card charges inclusive of all the charges incurred by the smart card holder through the Healthcare Exchange for the smart card holder in a single statement.

Fig. 6 shows the process flow of the transaction through the entire Healthcare exchange inclusive of Managed Care Plan insurer, credit card company, credit card insurer, payment network and MCO.

As in the case of Fig. 4 or 5, Fig 6 begins with the approach by

a smart card holder to a member of the Healthcare Exchange. The process would now be described in accordance to the steps identified at each stage involving the parties in this process.

1. Enrolment of Smart Card Holder

A smart card holder is required to sign a contract for at least a year to enroll their managed-care plans. Thereafter, MCO will arrange a X-months installment package for the smart card holder for the membership fee settlement, billed through the credit card accounts of the smart card holder.

The health coverage plan can also be structured in the form of number of clinical visit, health screening, etc. besides credit insured.

Disease management is a practice that treats high-risk, high-cost patients that have been diagnosed with chronic conditions for which there are broad variations in treatment. Online disease management will play a huge role in accelerating and simplifying this practice. With a Remote Health Monitor, the vital signs of a patient can be easily captured and transferred via the Internet to a centralized server. These data will be charted over a course of time in order to maintain a better control of the disease.

Generally, a remote health monitor costs between USD1000-00 to USD1500-00. The MCO will provide a X-months installment package billed through their credit card accounts.

By virtue of the MCO tying up with the Credit Card Company, the credit card account would have the benefit of allowing payment by installment (may be 0% interest rate due to promotion) for annual membership fee (or annual premium). The use of the credit card would also benefit the smart card holder in those expenses where the healthcare plan may not cover e.g. bill for clinical consultation or treatment not covered under managed-care plan subscribed; and payment for equipment.

2. Provision of services/goods by Healthcare Provider

On a visit to the Healthcare provider, the smart card holder would submit his smart card to the service provider for authentication and update of data.

A contact or contactless communication is then initiated between the identifier and its dedicated reader, followed by providing a password on a keypad or fingerprint on a bio-metric reader; Encrypted code B is stored in the memory of second identifier while encrypted code A and EMR are stored in the memory of first identifier. When a healthcare identifier is inserted/or swapped on its reader, encrypted code A will be sent from the memory to the database of MCO for an authentication process. Thereafter, if the authentication is successful, both EMRs stored in the card and in the database of MCO will be compared with respect to their dates of modification. Only the oldest record in the first Identifier of the smart card while the latest record will be uploaded and archived in the database of the Healthcare Exchange. The updates would include the credits if any, due to the smart card holder. If there is no available credits, the smart card holder would be informed by the service provider (through the MCO) that the service to be provided has to be settled by the smart card holder on his own account.

The use of the smart card would also enable the medical specialist to obtain the latest medical data on the smart card holder. After consultation, the latest EMR would be uploaded to and archived in the database of the MCO via the internet through the system of the service provider. This is to keep all histories relating to a patient (the smart card holder) as an audit trail in the database of the MCO. At the same time, a newer copy of the EMR would also be updated into the smart card simultaneously after the consultation.

3. Communication with Managed Care Organization ("MCO")

The contact or contactless communication initiated would have upon authentication resulted in updates of the data contained in the first identifier.

The data updated would include whether the smart card holder is entitled to any credits for services under the managed care plan to which he is a subscriber. If the smart card holder has credits, the healthcare provider would instantaneously be advised that the services to be provided is to be settled by the MCO. If not, the healthcare provider would be advised to inform the smart card holder that the services to be provided must be settled by the smart card holder on his own account.

4. Provision of financial services by Credit Card Company

If the data updated confirms that the smart card holder has no credits under his managed care plan, the health care provider would inform the smart card holder accordingly.

If the card holder has no credits under his managed care plan, he can still use first identifier to record his acquisition of service. There are also occasions when the smart card holder receives some service not covered under his managed care plan from some clinics or healthcare providers without any credit card reading facility. In this case, the smart card holder could use the smart card to record his acquisition of service. For such cases, after the provision of service, another contact or contactless communication would then be initiated, this time between the first identifier and its dedicated reader, followed by providing a password on a keypad or fingerprint on a bio-metric reader; Encrypted code A is stored in the memory of first identifier would be verified. The financial data from the transaction will be generated and stored by database of the MCO. Subsequently the same financial data would be transmitted by the MCO to the credit card center for billing consolidation. In this way, the sum charged for the service would be settled by the smart card holder in the usual procedure when the smart card holder receives his statement from his credit card company at the end of the billing cycle.

The present invention therefore offers the flexibility of using the smart card to acquire services from the healthcare provider when either the healthcare providers do not have any credit card reading facility or when the

smart card holder receives services not covered by his managed care scheme.

5. Role of Managed Care Plan Insurer

If the smart card holder has credits under his managed care plan, the MCO would submit the costs of the healthcare service to the Managed Care Plan Insurer for reimbursement.

6. Payment of Insurance Premium by MCO

In the course of each month, or periodically, as determined by agreement between the MCO and the Managed Care Plan Insurer, the MCO would pay the premiums for coverage of the Managed Care plan insurance scheme.

7. Generation of Member's record of transactions by MCO

Likewise, at the end of each billing cycle, the MCO would generate from its database a listing of all transactions accounted for by each smart card holder and which have been transmitted electronically during that period from each member of the Healthcare exchange XXXXX may be due to the smart card holder. The MCO would now send the details of the transactions of the smart card holder with the Healthcare Exchange to the Credit Card Company.

8. Generation of single statement by Credit Card Company

At the end of the billing cycle for the smart card holder, the credit card company would have received from all its own retailer members details of financial transactions for purchase of goods and service entered into by the smart card holder. A statement of all these financial transactions are then printed and sent to the smart card holder. The statement of financial transactions would list details of all charges agreed by the smart card holder including the charges incurred through

the Healthcare exchange.

If the smart card holder has credits for that month and no credit card charges was incurred in respect of his Healthcare policy, the statement from the Credit Card company would not reflect any charges from the Healthcare Exchange. The statement from the Credit Card company would now show the balance of any credit due to the smart card holder as at date of statement of the Credit Card Company.

Even though the smart card holder has credits and no credit card charges were incurred, it is still possible for some charges to be due e.g. installment of premium for managed care plan, purchase of equipment, installment due on purchase of remote health monitor programme. The smart card holder would therefore be able to see all the transactions with the Healthcare Exchange reflected in the credit card statement issued by the Credit Card Company, obviating the need for him to look at two statements.

9. Payment and Settlement

The smart cardholder receives bills from a provider (merchant) for an acquisition of its service or goods (paper/mail bills, email notices, implied bills for automatic debts), which indicate an amount, and a unique merchant identification number. To authorize a remittance, the cardholder transmits to his/her card issuer (usually a bank) a bill pay order indicating a payment date, a payment amount, the cardholder's account number with the merchant, a source of funds and the merchant identification number (or known as Biller Reference Number or " BRN "), either directly or by reference to static data containing those data elements. Merchant bank then submits a payment message to a Payment Network, and the Payment Network, which assigns the BRNs, forwards the payment message to the merchant bank.

When the monthly statement of all credit card transactions is issued to the smart card holder by the Credit Card Company, the smart card holder would be given an amount due for payment. The smart card

holder would now issue a cheque to settle the amount due. The cheque issued by the bank of the smart card holder would be paid over to the account of the credit card company. The credit card company would separately as part of its payment programme, pay to each retailer member including the healthcare provider, the credit card charges transacted at their outlets.

For settlement, the credit card company debits the cardholder's account and is obligated to a net position with the Payment Network. Likewise, the retailer's bank receives a net position from the Payment Network and credits the retailer's bank account. If the card issuer agrees to send non-reversible payment messages, the card issuer does not submit the transaction until funds are good unless the card issuer is willing to take the risk of loss if funds are not good, in the case of a guaranteed Payment Network. To share the risk, a card issuer will establish a policy with an insurer with an appropriate premium.

10. Sharing of credit risk

In line with current business practice, the credit risk of the credit card holders are insured with a credit insurer. Should a credit card holder or a smart card holder default, the credit card company would claim the default amount from the credit insurer.

11. Payment of premium for credit risk

To have the benefits of credit insurance, like any other insurance policy, the premium for such credit insurance must be paid by the credit card company.

It must be borne in mind that through the use of the first and second identifier in the smart card, the data arising from the visit to the healthcare provider is captured, and subsequently transferred from one member of the Healthcare Exchange to another member of the Healthcare Exchange such as the MCO and even to the Credit Card Company and Insurers without further data input. The use of the first and second identifier in the smart card within the Healthcare Exchange has potential

for substantial costs savings since there is no further requirement to convert data or manipulate the same data again.

Referring to Fig. 7, the smart card of the present invention can be used in any card reader installed in a plurality of devices or equipment and which is integrated with a healthcare identifier reader, and connected with a healthcare exchange. These devices could be a simple card reader module to be used in a retail shop selling healthcare equipment; in a medical clinic and in hospitals. Such devices can also be available in Public kiosk offering remote health monitoring services in which a smart card holder can obtain the latest data available on his healthcare or insurance plan. An example of such a remote health monitoring system has been disclosed in Singapore Patent Application No. 200205416-1 filed on 06.09.2002. Such device could also be made available in public transportation or connected to a computer module in a pharmacy. The devices could be connected to Daily appliances used for healthcare maintenance e.g. massage chairs and sofa chairs. Such devices would also be used for services offered on exercise machines e.g. treadmills. Another example of the device in use would be on portable monitoring device e.g. blood pressure, SPO2, blood glucose, pulse rate, body temperature and ECG. Another use of the device would be on electronic communication devices.

As described in the preceding paragraphs, the smart card holder can therefore check the information encrypted in the first Identifier in his smart card holder by using the smart card on any card reader integrated with the healthcare identifier reader. In the case where the smart card holder is medically unable to do so, the medical personnel attending to the smart card holder can place a telephone call to the 1800-xxxxxxx or 1900-xxxxxxx number printed on the back of the smart card. Such a call would be directed to a 24 X 7 call center and to request for detail of the medical/ health history of the cardholder. The helpdesk at the call center will be able to provide a full health or medical history relating to the cardholder through a web browser or fax machine after a secured authentication process over the telephone.

Alternatively, the emergency number printed on the smart card would enable the smart card holder to retrieve an "e-page" from a healthcare exchange through the web browser. During an emergency situation, this number can be used as the login number to access a summary page of predefined information relating to the cardholder, such as critical health data, allergy, next-of-kin's particulars, etc through a web browser. However, this emergency number is strictly for emergency situations.

Having described preferred embodiments of the invention with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments, and that various changes and modifications may be effected therein by one skilled in the art without departing from the scope or spirit of the invention as defined in the claims.

ADVANTAGEOUS EFFECTS OF THE INVENTION

The smart card of the present invention has a first identifier for authentication of an identity against a healthcare exchange over a secured network (Internet); and a memory to store electronic medical record. The second identifier provides for authentication of an identity against a credit payment network over a secured network (Internet). The identifiers would enable the smart card holder to carry out transactions with members of a Healthcare exchange as well as serve as a credit card. Thereafter the financial data relating to the transactions with all care providers are consolidated and sent to a financial institution such as credit card company for billing purposes. Use of the smart card offers the advantage in that the Credit Card Company issues a single billing statement which is then sent to the smart card holder.

The smart card would also has at least an emergency number (access code or the card number) which can be used as the login number to access a summary page of predefined information relating to the cardholder, such as critical health data, allergy, next-of-kin's particulars, etc through a web browser. In the present context, the summary page is named as "e-page".

The smart card has a 1800-xxx or 1900-xxx phone number which can be used in an emergency. This number is connected directly to a 24x7 call center, wherein during an emergency, the helpdesk will be able to provide a full health or medical history relating to the cardholder through a web browser or fax machine after a secured authentication process over the telephone.

CLAIMS

1. A smart card (10) operable with a card reader for use in a healthcare provider registered with a Healthcare Exchange (20), the smart card having:-

a first identifier (11) containing encrypted data ;

a second identifier (12) with credit card data of a smart card holder; and

a memory for storage, in encrypted code, an electronic medical record ("EMR") of the smart card holder

characterized in that the first identifier (11) is capable of authenticating the identity of the smart card holder against a database (21) in the Healthcare Exchange over a modem dial-up or dedicated network (Internet) access and the second identifier is capable of authenticating the identity of the smart card holder against a credit payment network over a modem dial-up or dedicated network (Internet) access during a transaction with the healthcare provider.

2. A smart card as claimed in Claim 1 having:-

an emergency number (13) which is either the access code or the card number which during an emergency situation, this number can be used as the login number to access a summary page of predefined information relating to the smart card holder, such as critical health data, allergy, next-of-kin's particulars, etc through a web browser; and

an 1800-xxx or 1900-xxx phone number (14) printed on the card for calling to a 24x7 call center, wherein during an emergency, the helpdesk will be able to provide a full health or medical history relating to the smart card holder through a web browser or fax machine after a secured authentication process over the telephone.

for use in an emergency encountered by the smart card holder either to obtain assistance from a healthcare provider registered with the Healthcare Exchange or from any medical institution.

3. A smart card (10) as claimed in Claim 1 wherein the first identifier (11) is a smart chip or a JAVA smart chip.

4. A smart card (10) as claimed in Claim 1 wherein the second identifier (12) containing credit card data of the smart card holder is a bar code, magnetic strip, smart chip or a JAVA smart chip issued by a Credit Card Company.

5. A smart card (10) as claimed in Claim 1 wherein the first identifier (11) stores the following data:-

general healthcare data including drug allergies and healthcare user's particulars including emergency contact number, body mass, height, blood group etc ;

Physician's advice and medical treatment of the last 5 to 30 clinical Visits or more;

Real time data gathered from the sensing modules includes blood pressure, pulse rate, blood glucose, body temperature, ECG and SPO2) of remote monitoring device; and

Encrypted password for identity authentication.

which upon successful authentication of the first identifier, the data stored in the first identifier (11) would be checked with the database (21) in the Healthcare Exchange for the latest update or vice versa; and the latest record will always only the oldest in the first Identifier (11) of the smart card while the latest record will be uploaded and archived in the database (21) of the Healthcare Exchange.

6. A smart card (10) as claimed in Claim 5 wherein upon successful authentication of the first identifier (11) with the Healthcare Exchange and upon the EMR stored in the Healthcare Exchange being compared with the EMR stored in the database (21) of the Healthcare Exchange, the updating of the EMR would include the financial information on transactions arising from use of the smart card including installments under managed care plans, purchases of supplies and services from service provider members of the Healthcare Exchange, purchases of medical services not covered by the managed care plans of the smart card holder and including any credits due to the smart card holder.

7. A smart card (10) as claimed in Claim 6 wherein the financial information on the transactions of the smart card with the Healthcare providers of the Healthcare Exchange are transmitted over a modem dial-up or dedicated network (Internet) access to the database (21) in the Healthcare Exchange and stored in the said database and at the end of a billing cycle, the financial information on the transactions of the smart card are sent to the Credit Card Company and the said financial information is consolidated with other financial information on transactions made by the smart card holder using the second identifier of the smart card or another credit card or a debit card issued by the same Credit Card Company.

8. A smart card (10) as claimed in Claim 7 wherein the financial information on the transactions with healthcare providers of the Healthcare Exchange using the first identifier of the smart card and financial information on transactions of the second identifier of the smart card and other credit cards or debit cards of the smart card holder are consolidated by the same Credit Card Company which issued the second identifier, the financial information being presented in one consolidated billing statement issued by the Credit Card Company and sent to the smart card holder for settlement by the smart card holder.

9. A smart card (10) as claimed in Claim 1 operable with a card reader installed in a Public Kiosk offering remote health monitoring services or a card reader installed in a personal computer or a note book or a

PDA or e-tablet or mobile phone and which is connected by a modem dial-up or dedicated network (Internet) access wherein upon successful authentication of the first identifier, the smart card holder would be able to access a website of the Healthcare Exchange, for information on the EMR of the smart card holder, access Telemedicine services, On-line Disease management, Healthcare applications such as billing status, making of appointments with healthcare providers and making of general enquiries and access to Healthcare user education and programmes for health maintenance .

10. A smart card (10) as claimed in Claim 1 operable with a card reader installed in a device operated by a healthcare provider registered with the Healthcare Exchange or in a device installed in a public kiosk wherein the device could be a remote monitoring device, a massage chair or a treadmill and the smart card holder would receive healthcare service such as monitoring of blood pressure, pulse rate, blood glucose, body temperature, ECG and SPO2, or massage or a heart check.

11. A smart card (10) as claimed in Claim 1 operable with a card reader installed in a Public Kiosk offering remote health monitoring services or a card reader installed on a personal computer or in a note book or a PDA or e-tablet or mobile phone and which is connected to the Internet wherein upon successful authentication of the first identifier, the smart card holder can view the latest data available on the smart card holder's managed care plans or health insurance plans over the Internet.

12. A smart card (10) as claimed in Claim 1 operable with a card reader installed in a device operated by a healthcare provider registered with the Healthcare Exchange wherein the smart card could be used to receive medical care services such as hospital stay and treatment, nursing care, pharmaceutical supplies, medical treatment and consultation by medical specialists and general practitioners, nutritional food and healthcare products, supplies from healthcare library, suppliers of medical devices and equipment, laboratory tests reports and other services undertaken by Healthcare Exchanges.

13. A smart card (10) as claimed in Claim 1 for use with a healthcare provider without a card reader installed by a payment network whereby the first identifier in the smart card is used on the card reader and upon authentication, the financial information arising from the transaction with the healthcare provider is transmitted over a modem dial-up or dedicated network (Internet) access to the database (21) in the Healthcare Exchange and stored in the said database and at the end of a billing cycle, the said financial information is sent to the Credit Card Company and consolidated with other financial information on transactions made by the smart card holder using the second identifier of the smart card or another credit card or a debit card issued by the same Credit Card Company.

14. A smart card (10) as claimed in Claim 1 which can be used as a credit card.

15. A system for capturing financial information arising from transactions using a smart card (10) as claimed in Claim 1 wherein the financial information is transmitted over a modem dial-up or dedicated network (Internet) access from the card reader installed in the healthcare provider to the database (21) of the Healthcare Exchange and at the end of a billing cycle, the financial information are sent by the Healthcare Exchange (20) to the Credit Card Company which issued the second identifier (12) and thereafter, the said financial information is consolidated by the same Credit Card Company with other financial information received by the same Credit Card Company on transactions made by the smart card holder using the second identifier of the smart card or another credit card or a debit card issued by the same Credit Card Company to the same card holder.

16. A system for capturing data stored in a first identifier of a smart card as claimed in Claim 1 operable with a card reader used by a healthcare provider registered with a Healthcare Exchange or with a card reader installed in devices such as Personal Computer or a PDA or e-tablet or mobile phone or in a device installed in a public kiosk offering remote health monitoring services or in a device installed in a massage chair or in a treadmill, said first identifier being capable of authenticating

the identity of the smart card holder against a database (21) in the Healthcare Exchange over a modem dial-up or dedicated network (Internet) access, wherein upon successful authentication of the first identifier, the data stored in the first identifier (11) would be checked with the database (21) in the Healthcare Exchange for the latest update or vice versa; and the latest record will always replace only the oldest in the first Identifier (11) of the smart card while the latest record will be uploaded and archived in the database (21) of the Healthcare Exchange.

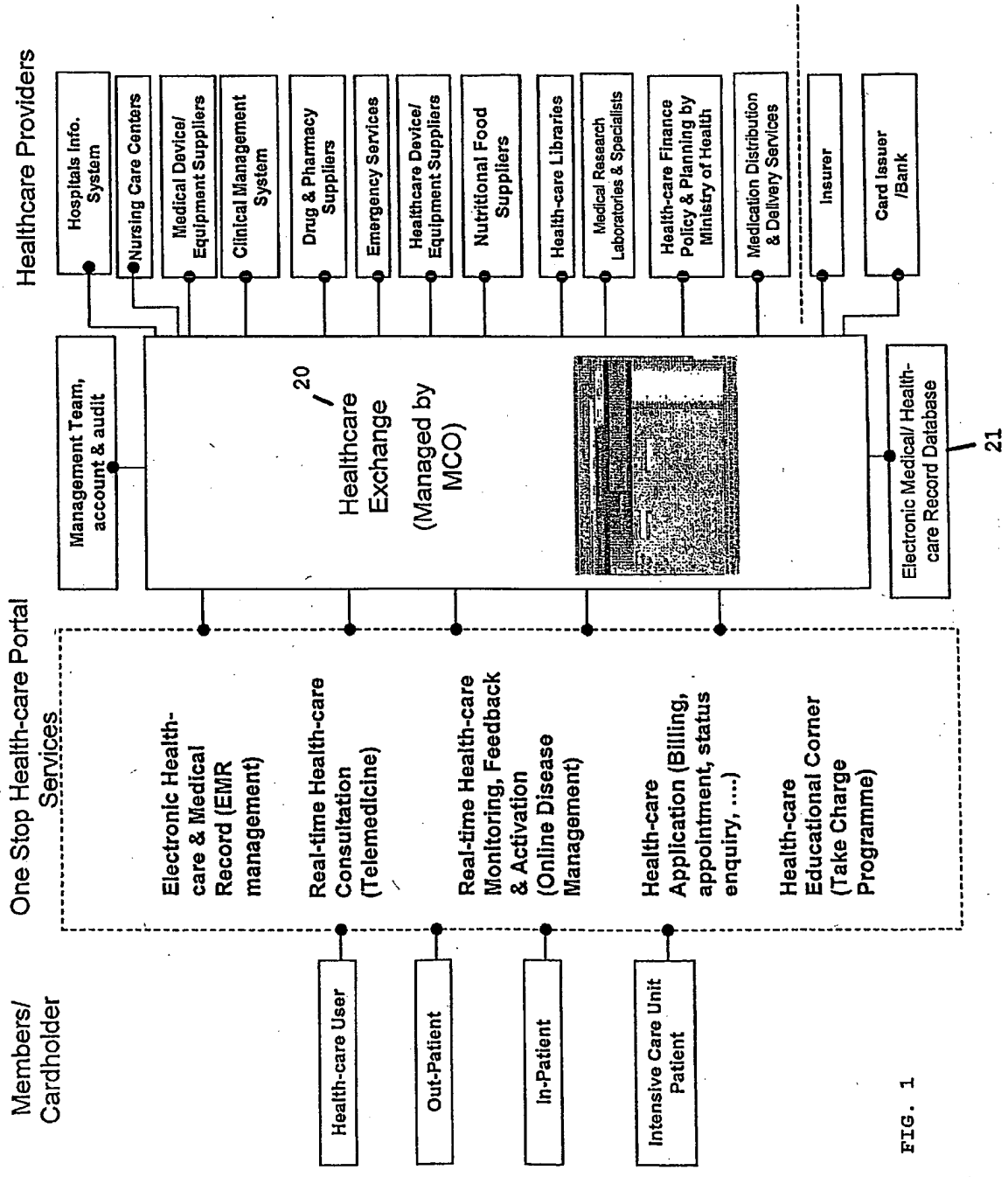
Healthcare Providers
Hospitals Info. System
Nursing Care Centers
Medical Device/ Equipment Suppliers
Clinical Management System
Drug & Pharmacy Suppliers
Emergency Services
Healthcare Device/ Equipment Suppliers
Nutritional Food Suppliers
Health-care Libraries
Medical Research Laboratories & Specialists
Health-care Finance Policy & Planning by Ministry of Health
Medication Distribution & Delivery Services
Insurer
Card Issuer /Bank
Management Team, account & audit
20
Healthcare Exchange (Managed by MCO)
Electronic Medical/ Health-care Record Database
21
One Stop Health-care Portal Services
Electronic Health-care & Medical Record (EMR management)
Real-time Health-care Consultation (Telemedicine)
Real-time Health-care Monitoring, Feedback & Activation (Online Disease Management)
Health-care Application (Billing, appointment, status enquiry, ...)
Health-care Educational Corner (Take Charge Programme)
Members/ Cardholder
Health-care User
Out-Patient
In-Patient
Intensive Care Unit Patient

FIG. 1

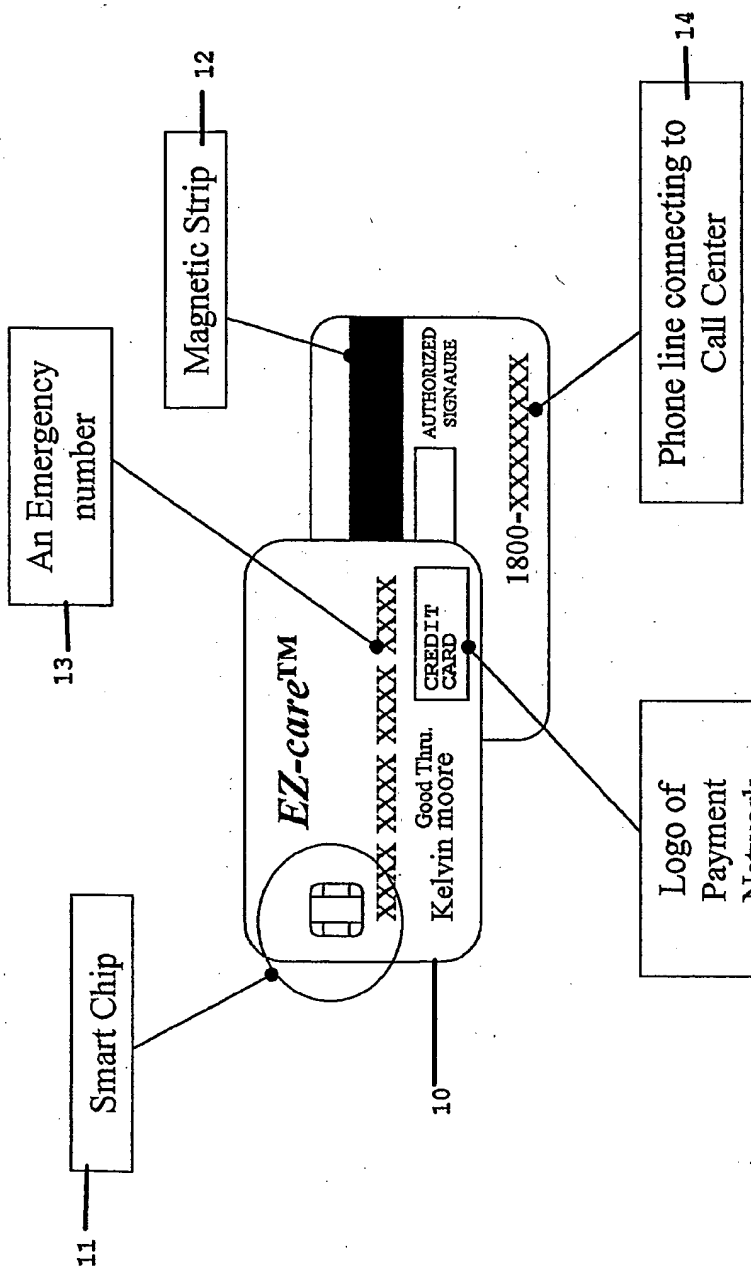
An Emergency number
13
Magnetic Strip
12
Phone line connecting to Call Center
14
AUTHORIZED SIGNAURE
1800-XXXXXXXX
EZ-care™
XXXX XXXX XXXX XXXX
Good Thru.
Kelvin moore
CREDIT CARD
Logo of Payment Network
Smart Chip
11
10

Fig 2

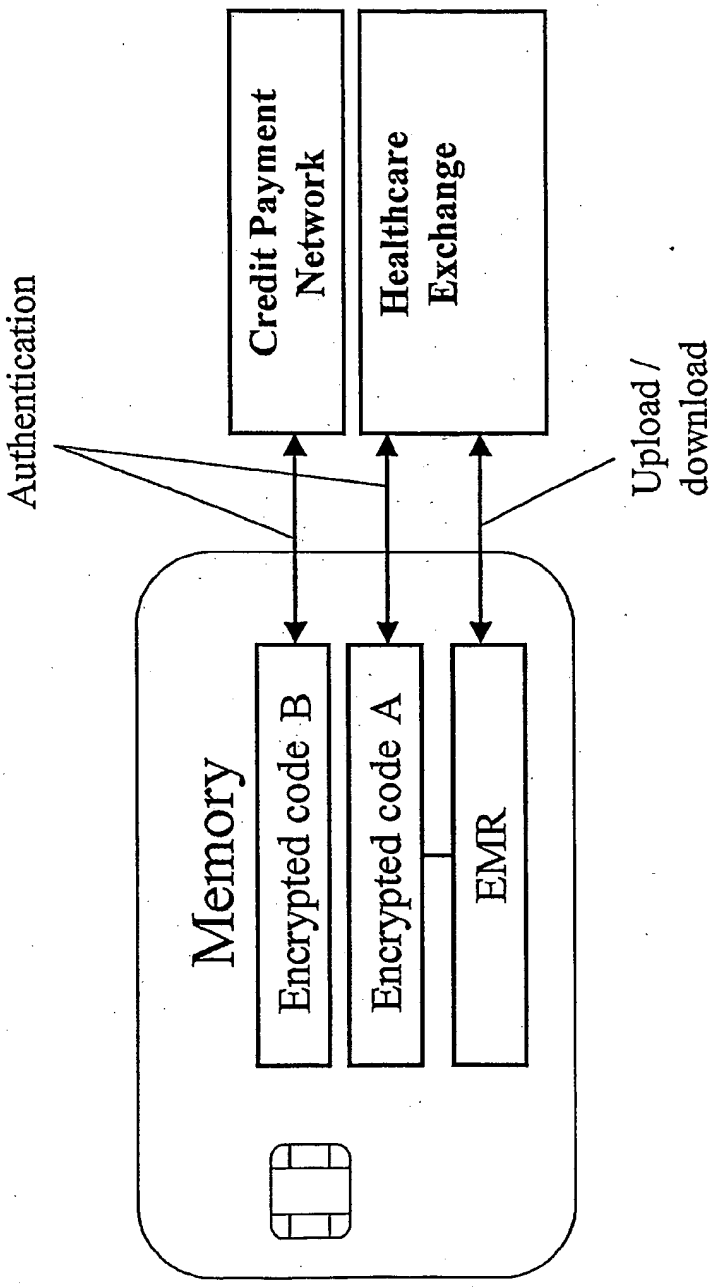
Credit Payment Network
Healthcare Exchange
Authentication
Upload / download
Memory
Encrypted code B
Encrypted code A
EMR

Fig 3

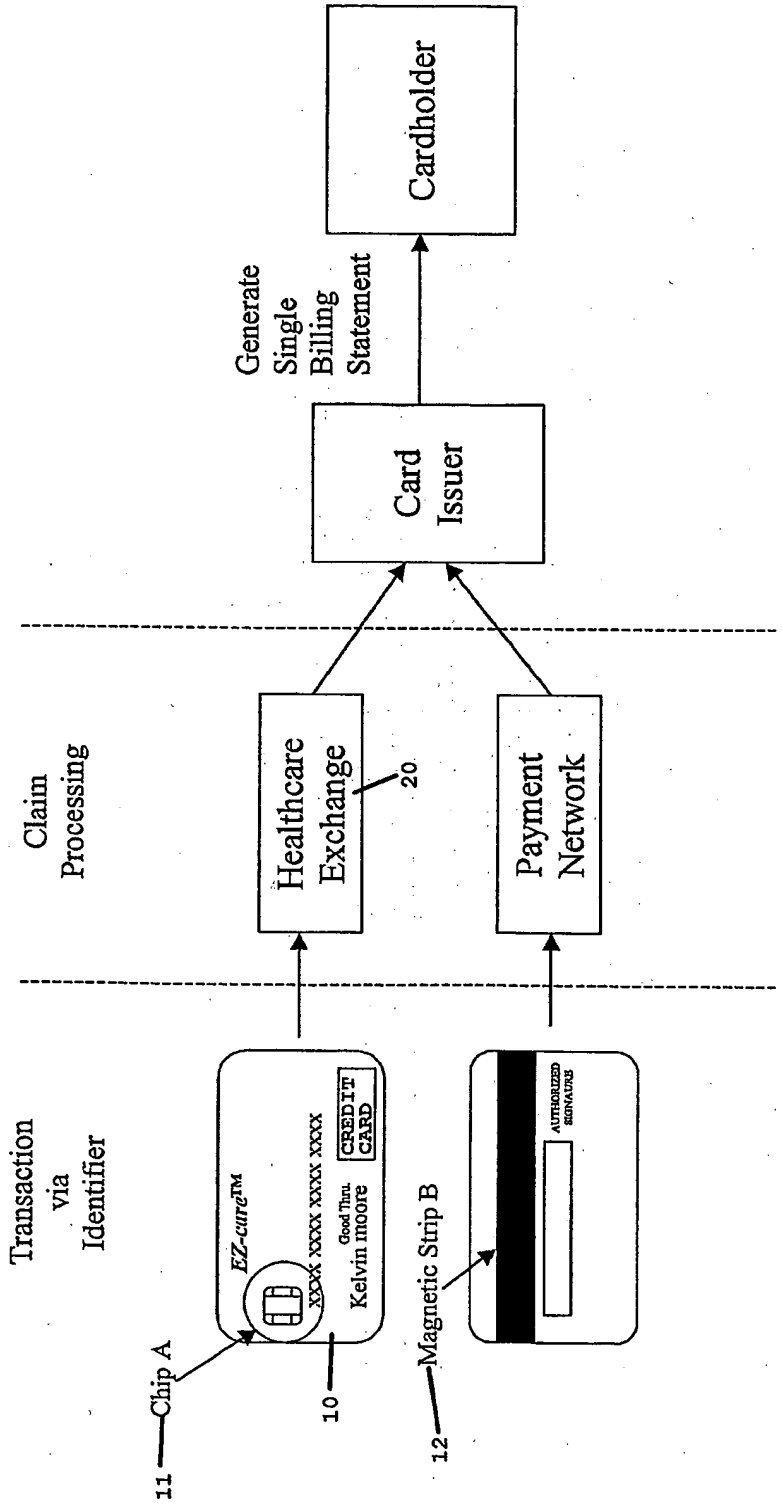
Cardholder
Generate Single Billing Statement
Card Issuer
Claim Processing
Healthcare Exchange
20
Payment Network
Transaction via Identifier
EZ-care™
XXXX XXXX XXXX XXXX
Good Thru
Kelvin moore
CREDIT CARD
AUTHORIZED SIGNATURE
Chip A
11
10
Magnetic Strip B
12

Fig 4

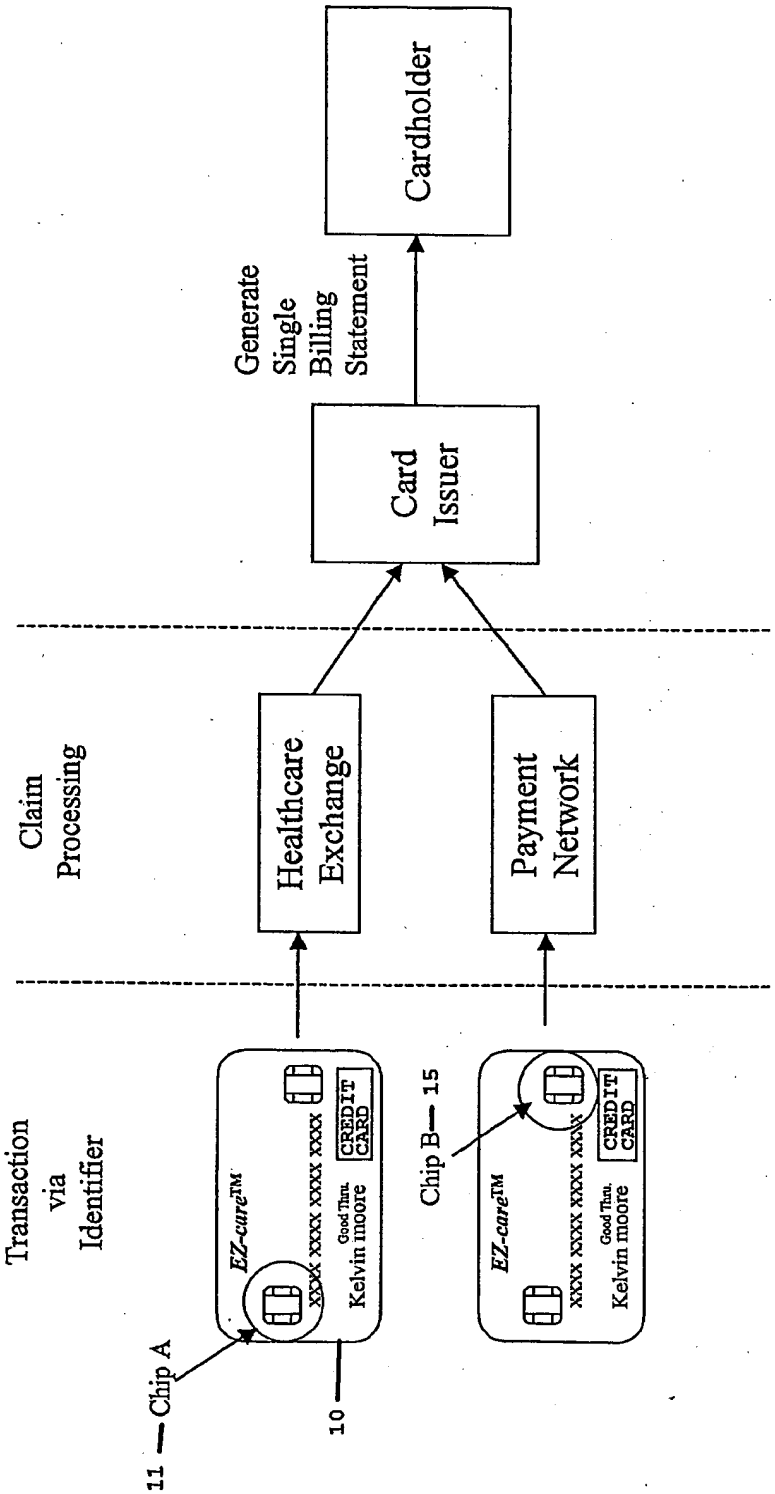
Transaction via Identifier
Claim Processing
Healthcare Exchange
Payment Network
Card Issuer
Generate Single Billing Statement
Cardholder
Chip A
11
10
Chip B
15
EZ-care™
XXXX XXXX XXXX XXXX
Good Thru
Kelvin moore
CREDIT CARD

Fig 5

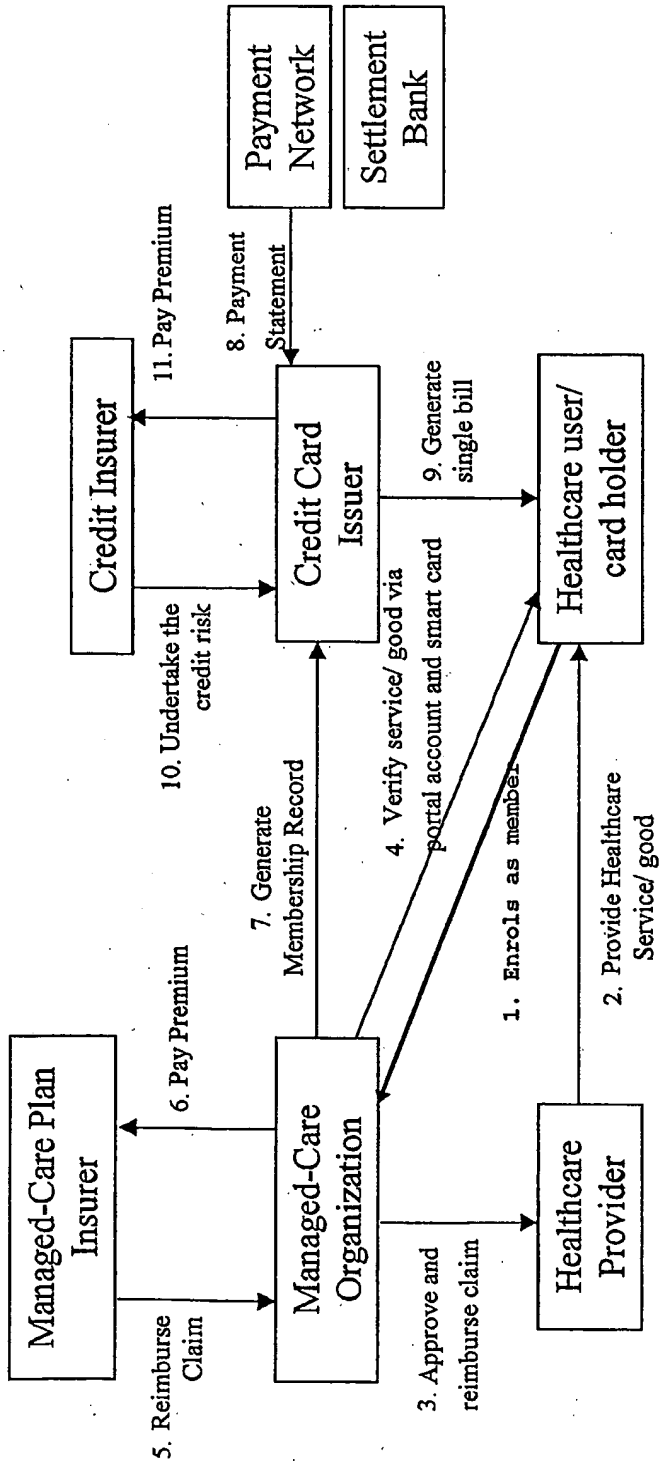
Payment Network
Settlement Bank
Credit Insurer
Credit Card Issuer
Healthcare user/ card holder
Managed-Care Plan Insurer
Managed-Care Organization
Healthcare Provider
11. Pay Premium
8. Payment Statement
10. Undertake the credit risk
9. Generate single bill
4. Verify service/ good via portal account and smart card
7. Generate Membership Record
1. Enrols as member
6. Pay Premium
2. Provide Healthcare Service/ good
5. Reimburse Claim
3. Approve and reimburse claim

Fig 6

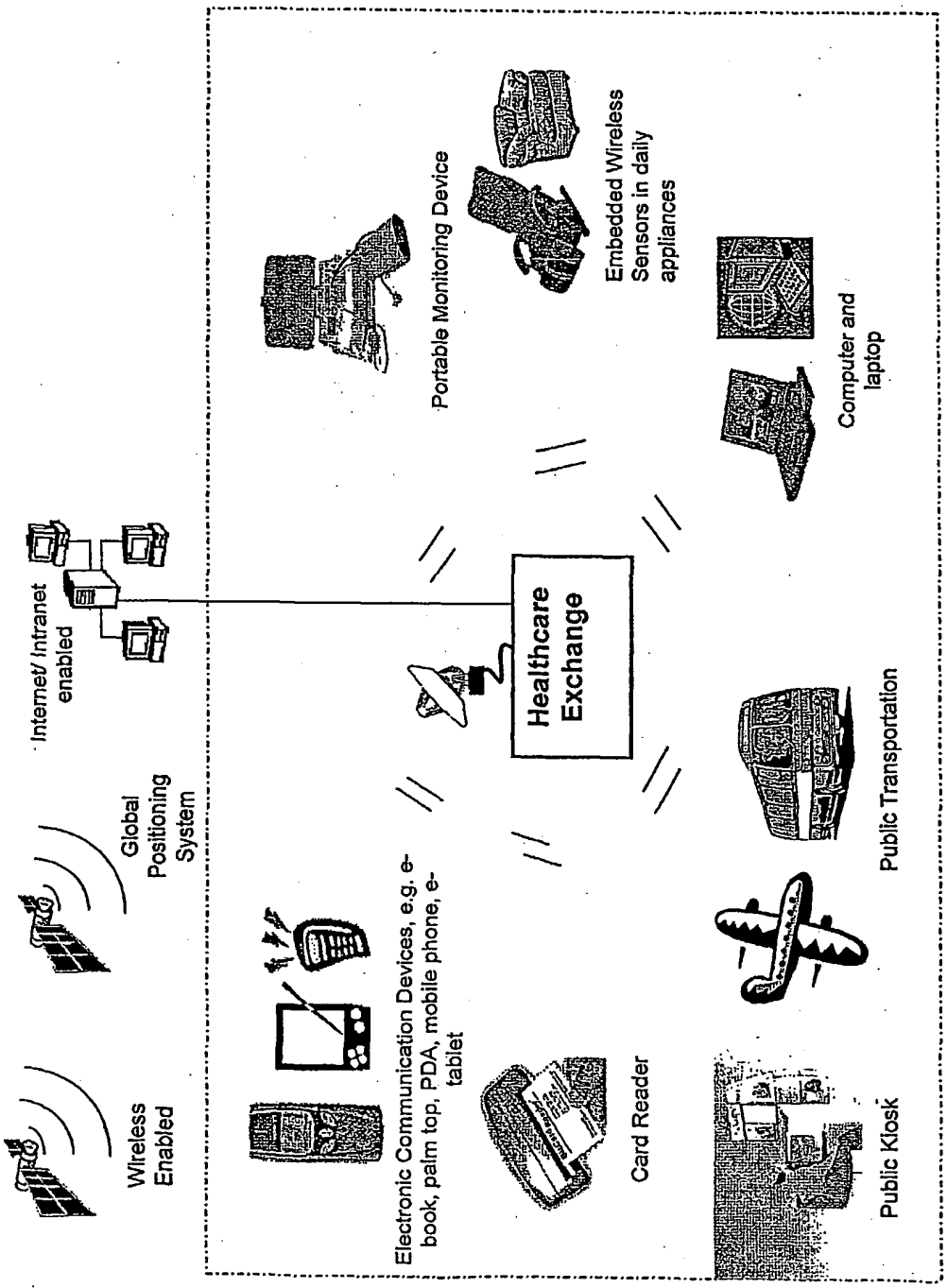
Internet/ Intranet enabled
Global Positioning System
Wireless Enabled
Electronic Communication Devices, e.g. e-book, palm top, PDA, mobile phone, e-tablet
Card Reader
Public Kiosk
Healthcare Exchange
Portable Monitoring Device
Embedded Wireless Sensors in daily appliances
Computer and laptop
Public Transportation

Fig 7